UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,057	08/30/2001	Gregor P. Freund	VIV/0003.01	8336

28653 7590 01/22/2009

JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

EXAMINER	
DIVECHA, KAMAL B	

ART UNIT	PAPER NUMBER
2451	

MAIL DATE	DELIVERY MODE
01/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/944,057
Filing Date: August 30, 2001
Appellant(s): FREUND ET AL.

John A. Smart
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/7/08 appealing from the Office action mailed 5/5/08.

(1) Real Party in Interest

The statement containing the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Stockwell et al., US 5,950,195, issued on Sep. 7, 1999, and filed on Sep. 18, 1996

Phillips et al., US 6,721,555 B1, issued on Apr. 13, 2004, and filed on Feb. 18, 2000

Kadyk et al., US 6,996,841 B2, issued on Feb. 7, 2006, and filed on Apr. 19, 2001

Shrader et al., US 6,026,440, issued on Feb. 15, 2000, and filed on Jan. 27, 1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-5, 7-12, 17-22, 24, 27-29, 31-33, 35-39, 45-55, 57 and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Philips, US 6,721,555 B1).

As per claim 1, Stockwell discloses a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (fig. 1: the computers connected to internal network, col. 4 L21-42: a firewall gateway), a method for managing Internet access based on a specified access policy (col. 1 L5-10, col. 3 L16-54, col. 5 L16-22: access policies), the method comprising:

a challenge/response sequence, i.e. transmitting a challenge and receiving a response, for determining whether a given client computer is in compliance with said specified access policy (col. 5 L16 to col. 6 L67, col. 8 L38 to col. 9 L60: authentication is type of rule/policy that governs Access);

blocking Internet access for any client computer that does not respond appropriately to any challenge issued to it (col. 5 L16 to col. 6 L67, col. 9 L1-60: blocking the Internet access by dropping the connection, col. 11 L5-67);

reassessing the connection based on time intervals, i.e. reassessing the connection over period of time by reissuing ACL checks that comprises authentication, i.e. challenge/response sequence (col. 9 L61 to col. 10 L8).

However, Stockwell does not explicitly disclose the process of transmitting plurality of challenges over a period of time from said client premises equipment to each client computer **for** determining whether a given client computer remains in compliance with policy during period of time and transmitting a response from at least one client computer back to said client premises equipment **for** responding to each of challenges that has been issued.

Philips explicitly discloses an Internet access device that performs the process of transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer for determining whether the given client computer remains in compliance and transmitting a response from at least one client computer back to said client premises equipment for responding to each of said challenges that has been issued (col. 4 L50-67, col. 5 L6 to col. 6 L28, col. 7 L4-9: IFW with router).

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Stockwell in view of Philips in order transmit a plurality of challenges over period of time to the client computer and receiving a response to the challenges.

One of ordinary skilled in the art would have been motivated because it would have provided a mechanism for periodically verifying the users and/or clients, thus improving security (Phillips: col. 5 L19-64).

As per claim 2, Stockwell discloses the process wherein a client computer that does not respond at all is blocked from Internet access (col. 5 L16 to col. 6 L67, col. 9 L1-60: blocking the Internet access by dropping the connection; its also obvious that if the client doesn't respond to the username/pswd-login prompt, the client will not be allowed to access the Internet).

As per claim 3, Stockwell discloses the process wherein a client computer that responds with a particular predefined code indicating non-compliance is blocked from Internet access (i.e. invalid response, col. 5 L16 to col. 6 L67, col. 9 L1-60: its obvious that if client responds to the challenge with incorrect information or code, the client will be blocked or not allowed to access the Internet).

As per claim 4, Stockwell discloses the process wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access (col. 5 L16 to col. 6 L67, col. 9 L1-60).

As per claim 5, Stockwell discloses the process wherein before a receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment for requesting the client premises equipment to transmit a challenge to that particular client computer (i.e. transmitting an initial connection request message that enables the firewall to send the challenge, col. 5 L53 to col. 6 L67, col. 8 L38 to col. 9 L60, col. 14 L5-55).

As per claim 7, Stockwell discloses the process wherein client premises equipment is capable of permitting Internet access by selected client computers and denying access to other

client computers (col. 10 L12 to col. 11 L46, col. 11 L47 to col. 13 L67: several examples of ACLS, col. 8 L38-45).

As per claim 8, Stockwell disclose the process wherein access policy specifies rules that govern Internet access by the client computers (fig. 5, col.1 L40 to col. 2 L67, col. 5 L16-46, col. 6 L46 to col. 7 L67, col. 10 L12 to col. 11 L67).

As per claim 9, Stockwell discloses the process of determining whether permitting Internet access for a given client computer would violate any of rules and if permitting such Internet access would violate any of said rule, denying Internet access for that client computer (fig. 5, col.1 L40 to col. 2 L67, col. 5 L16-46, col. 6 L46 to col. 7 L67, col. 10 L12 to col. 11 L67: its obvious that this determination will be made in order to deny or allow the Internet access).

As per claim 10, Stockwell discloses the process wherein access policy includes rules that are enforced against selected ones of users, computers and groups thereof (col. 10 L12 to col. 11 L67).

As per claim 11, Stockwell discloses the process wherein said access policy specifies which applications are allowed Internet access (col. 5 L16-22, col. 7 L1-45, col. 8 L20-30: ftp and http type of accesses, col. 10 L12-67: Matching criteria for rule including: a list of service names such as ftp or http, in other words, a list of applications).

As per claim 12, Stockwell discloses the process wherein said access policy specifies applications that are allowed Internet access (col. 5 L16-22, col. 7 L1-45, col. 8 L20-30: ftp and http type of accesses, col. 10 L12-67: Matching criteria for rule including: a list of service names such as ftp or http, in other words, a list of applications).

As per claim 17, Stockwell discloses the process wherein said access policy specifies Internet access activities that are permitted or restricted for applications or version thereof (col. 5 L16-22, col. 7 L1-45, col. 8 L20-30: for http, types of URLs blocked, col. 10 L12-67, col. 11 L35-41, col. 14 L13-24).

As per claim 18, Stockwell discloses the process wherein said access policy specifies rules that are transmitted to client computers from a remote location (col. 8 L38 to col. 9 L60, col. 11 L5-67).

As per claim 19, Stockwell discloses the process wherein the remote location comprises a centralized location for maintaining said access policy (col. 5 L35-46, col. 7 L1-67, col. 8 L38 to col. 9 L60, col. 11 L5-67: a relational database).

As per claim 20, Stockwell discloses the process wherein the process of blocking Internet access includes determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group thereof (col. 5 L16 to col. 6 L67, col. 7 L1-67, col. 8 L38 to col. 9 L1-60, col. 10 L12 to col. 11 L67, col. 13 L11 to col. 14 L55).

As per claim 21, Stockwell discloses the process wherein challenge includes a request for a particular client computer to respond as to whether it is in compliance with said access policy (col. 5 L16 to col. 6 L67, col. 9 L1-60).

As per claim 22, Stockwell discloses the process of redirecting a client computer that is not in compliance with said access policy to a sandbox server (i.e. a server, col. 7 L45 to col. 8 L20, col. 11 L5 to col. 12 L44) and informing client computer that it is not in compliance with

said access policy (col. 9 L1 to col. 10 L8: sending a warning message to the client in response to denied connection).

As per claim 46, Stockwell discloses the system wherein said client premises equipment includes a router (col. 4 L8-42).

As per claim 47, Stockwell discloses the system wherein said access policy is provided at client computer to be regulated (col. 3 L18-54, col. 5 L16-67).

As per claim 48, Stockwell discloses the system wherein enforcement module is provided at client premises equipment (fig. 2, col. 4 L21-42, col. 5 L16-67).

As per claims 24, 27-29, 31-33, 35-39, 45, 49-55, 57, 61, they do not teach or further define over the limitations 1-5, 7-12, 17-22, 46-48. Therefore claims 24, 27-29, 31-33, 35-39, 45, 49-55, 57, 61 are rejected for the same reasons as set forth in claims 1-5, 7-12, 17-22, 46-48.

Claims 6 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Philips et al. (hereinafter Philips, US 6,721,555 B1), and further in view of Kadyk et al. (hereinafter Kadyk, US 6,996,841 B2).

As per claim 6, Stockwell in view of Phillips does not disclose the process wherein the initial message comprises a “client hello” packet.

Kadyk explicitly discloses the process of sending the “client hello” packet to the server (fig. 3A, col. 10 L20-52).

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Stockwell in view of Phillips and further in view of Kadyk in order send a client hello packet.

One of ordinary skilled in the art would have been motivated because it would have created a secured session (Kadyk: col. 10 L20-52).

As per claim 30, it does not teach or further define over the limitations in claim 6. Therefore claim 30 is rejected for the same reasons as set forth in claim 6.

Claims 13-16, 34, 42-44, 56 and 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Philips et al. (hereinafter Philips, US 6,721,555 B1), and further in view of "Official Notice".

As per claim 13, Stockwell in view of Phillips disclose the process wherein the applications are specified by executable name (col. 13 L10-67, col. 12 L10-67).

However, Stockwell in view of Phillips does not disclose the process wherein the applications are specified by version number.

But, application name and the version number are two common parameters used in the art for identifying applications.

Therefore, Official Notice is taken to indicate that specifying the applications by executable name and version number is well-known in the art.

As such, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Stockwell and Phillips in order to use the executable name and version number of the applications.

One of ordinary skilled in the art would have been motivated because these are common parameters used for identifying the applications.

As per claims 14-16, Stockwell in view of Phillips does not disclose the process wherein the applications are specified by digital signatures, wherein the digital signatures are computed using cryptographic hash, and wherein the cryptographic hash comprises one of Secure Hash algorithm (SHA-1) and MD5 cryptographic hashes.

But, Secure Hash algorithm (SHA-1) and MD5 cryptographic hashes, digital signatures are all well-known in the art, as explicitly admitted by the applicant (see specification, pg. 29 lines 14-31, pg. 10 lines 24-41).

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Stockwell and Phillips in order to specify the applications using hashing techniques.

One of ordinary skilled in the art would have been motivated because it would have provided secure communications.

As per claims 34, 42-44, 56 and 58-60, they do not teach or further define over the limitations in claims 13-16. Therefore, claims 34, 42-44, 56 and 58-60 are rejected for the same reasons as set forth in claims 13-16.

Claims 23, 25, 26, 40, 41 and 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Philips et al. (hereinafter Philips, US 6,721,555 B1), and further in view of Shrader et al. (hereinafter Shrader, US 6,026,440).

As per claim 23, Stockwell in view of Phillips discloses the process of redirecting the client computer that is not in compliance with said access policy to a particular port on the sandbox server (i.e. an alternate machine or server, col. 7 L45 to col. 8 L20, col. 11 L5 to col. 12 L44).

However, Stockwell in view of Phillips does not disclose the process of displaying error message pages on the sandbox server in response to communications on particular ports.

Shrader explicitly discloses the process of displaying error messages on a server if the request fails (col. 4 L40-67, obviously the request will fail on a particular machine or port, in this case at the web server port).

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Stockwell in view of Phillips and further in view of Shrader in order to display the error messages on the sandbox server or alternate server.

One of ordinary skilled in the art would have been motivated because it would have notified the client computer of the denial of the service (Shrader, col. 4 L56-667). It would have also improved the routers performance by redirecting the unauthorized client computers to alternate server.

As per claim 26, Stockwell in view of Phillips does not disclose the process wherein after displaying error message, permitting said client to elect to access the Internet.

Shrader discloses the process of displaying the error in response to inappropriate credentials and allowing the client to elect or to access the Internet by prompting the user (col. 4 L56-67).

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Stockwell in view of Phillips and further in view of Shrader in order to enable the client to elect to access the Internet.

One of ordinary skilled in the art would have been motivated because it would have provided the client computer another opportunity to access the Internet.

As per claims 25, 40, 41 and 62-64, they do not teach or further define over the limitations in claims 23 and 26. Therefore claims 25, 40, 41 and 62-64 are rejected for the same reasons as set forth in claims 23 and 26.

(10) Response to Argument

Examiner summarizes various issues raised by the appellant and addresses each of them separately.

In the Brief, appellant argues the:

a. 35 USC 103 rejections based on Stockwell and Phillips (Brief, pg. 7-14 [A]: First Ground).

In response to appellant's argument [a], Examiner respectfully disagrees.

Initially, appellant begins with "At its core architectural level, appellant's invention is fundamentally different from the combination of Stockwell with Phillips. By way of brief review, appellant's invention includes a router-side client management protocol (CMP) installed and operational on the client's (i.e. the user's) router (client premises equipment). This operates in...that is installed and running on the user's computers. This security module continually enforces compliance with an access or security policy (i.e. rules set by an organization, for

establishing permitted access activities of a user's computer)…." e.g. brief, pg. 9-10: Last paragraph.

Appellant's Independent claim 1 is reproduced herein:

> In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
> transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer, **for** determining whether a given client computer remains in compliance with said specified access policy during said period of time;
> transmitting a response from at least one client computer back to said client premises equipment for responding to each of said challenges that has been issued; and
> blocking Internet access for any client computer that does not respond appropriately to any challenge issued to it.

Appellant's Independent claim 24 is reproduced herein:

> In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
> transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy during said period of time;
> transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued; and
> redirecting a request for Internet access by any client computer that does not respond appropriately to any challenge issued to it to a sandbox server.

Appellant's Independent claim 45 is reproduced herein:

> A system for regulating Internet access by client computers comprising:
> an access policy governing Internet access by said client computers;
> client premises equipment serving a routing function for each client computer to be regulated and capable of issuing a plurality of challenges over a period of time to each client computer, for determining whether a given client computer is in compliance with said access policy during said period of time;
> one or more client computers which can connect to the Internet and at least one of which can respond to challenges issued by said client premises equipment; and
> an enforcement module for selectively blocking Internet access to the Internet for any client computers that fail to respond in a manner that would establish that they are in compliance with said access policy.

Clearly, the claims fail to disclose the appellant's core architectural level components such as client-side security module that is installed and running on the user's computers. Furthermore, the claim also fails to disclose "this security module continually enforces compliance with an access or security policy" as asserted by the appellant in the brief.

Appellant throughout the prosecution fails to note that:

During patent examination, the pending claims must be "given >their< broadest reasonable interpretation consistent with the specification." > In re Hyatt, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000). **Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).**

Appellant is, impermissibly, reading and/or importing the disclosure and/or specification into the claims, and has made this a basis throughout the brief in an attempt to differentiate the combination of Stockwell and Phillips with the claimed invention, as shown below.

At best, the claim discloses client premises equipment, i.e. a router or a firewall, sending plurality of challenges over a period of time **for** determining whether a given client computer remains in compliance and/or is in compliance with said specified access policy during said period of time, sending a response from at least one client computer back to the client premises equipment, i.e. response can be from user operating the computer, and blocking Internet access for any client computer that does not respond appropriately to any challenge.

A challenge, in view of appellant's specification, e.g. pg. 33 lines 2-5, is a packet and/or data sent to an individual client computer or to all client computers expecting a response to

permit Internet access. The packet and/or data can be a login prompt that asks the user of the computer for username and password.

Stockwell et al.

Stockwell discloses a system and method for regulating the flow of internetwork connections, i.e. Internet access, see fig. 4, through a firewall, see fig. 1, reproduced herein.

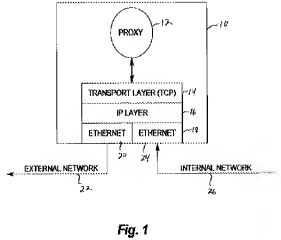

Fig. 1

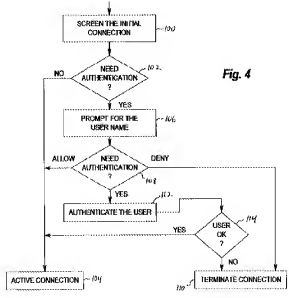

Fig. 4

Stockwell also discloses the usage of ACLs, **access control lists which is a list of rules that regulate the flow of Internet connections through a firewall**. These rules control how a firewalls server and proxies will react to connection attempts. When a server receives an incoming connection, it performs an **ACL check on that connection**, as evidenced by the following section (col. 5 L17-35):

As noted above, an Access Control List, or ACL, is a list of rules that regulate the flow of Internet connections through a firewall. These rules control how a firewall's servers and proxies will react to connection attempts. When a server or proxy receives an incoming connection, it performs an ACL check on that connection.

An ACL check compares a set of parameters associated with the connection against a list of ACL rules. The rules determine whether the connection is allowed or denied. A rule can also have one or more side effects. A side effect causes the proxy to change its behavior in some fashion. For example, a common side effect is to redirect the destination IP address to an alternate machine. In addition to IP connection attempts, ACL checks can also made on the console logins and on logins made from serial ports. Finally, ACL checks can also be made on behalf of IP access devices, such as a Cisco box, through the use of the industry standard TACACS+ protocol.

This ACL list is created by the administrator as follows (col. 6 L46-67):

The system administrator is responsible for creating the ACL ruleset. The ACL ruleset is a reflection of the administrator's security policy. The administrator needs to answer the following questions before creating the ruleset:

1) Where are the boundaries of the security domains?
2) Which security domains should be allowed to initiate connections into other security domains?
3) What types of information should be allowed to flow between the security domains?
4) Should connections be allowed based on host name, user name, time of day, or some combination thereof?
5) What type(s) of user authentication, if any, should be required to enter a security domain?

In the preferred embodiment, the ACL ruleset can be modified by the administrator using either a graphical user interface, or GUI, or a command line interface. Changes to the ACL ruleset are stored in the internal database. To prevent the occurrence of transient states that may violate the security policy, the database is locked during periods in which the administrator is making more than one rule update. (This is especially important when reloading the entire database from diskette or tape.)

More specifically, when the connection attempt is received, the ACL check procedure is performed as follows (col. 8 L38 to col. 9 L4):

ACL Check Procedure

The steps followed in executing an ACL check are shown in FIG. **4**. In FIG. **4**, the process starts at **100** where an agent can perform an optional initial ACL check when a connection is first detected. Most agents will perform an initial ACL check when a connection is first detected. The reason is that connections from some hosts are always disallowed. In this case the connection should be rejected with no further action. For most proxies and servers, Network Services Sentry (NSS) **70** will screen out the initial connection.

Note: If the agent is incapable of doing authentication (e.g., gopher or WAIS), NSS **70** should set the selected warder to "none" before it does the initial check. This avoids a potential ambiguity created by a tentative check on an unknown user name (explained later).

Some agents, such as ftpd, listen for connections directly and do not depend on NSS. These agents have to make the initial check themselves.

If the reply to the initial check says "deny" the connection should be closed at that point and no further communication should occur. If the initial check says "allow" the agent can proceed to step **102**. As we shall see below, "allow" really means "maybe" until further information about the user is obtained.

If the reply to the initial check says "allow," at **102** the agent should examine the reply to see if it demands authentication of the user. Note that if the agent was screened by NSS **70**, the agent will have to issue a duplicate check to get the ACL information because NSS **70** does not pass the ACL information to the agent.

If the ACL reply does not demand authentication, the ACL check procedure is complete and the agent can proceed to **104** to open the connection. Note that some servers, such as ftpd, will always demand authentication anyway.

In other words, one of the rules set by administrator is that the user must be authenticated and/or authorized to access the connection, and/or whether the authentication is need, and requires the user to perform and/or follow the authorization procedure before the access can be granted, e.g. fig. 4 step 108, 112.

If the authentication is demanded and/or needed, which is determined through ACL check procedure, **In step 112**, a challenge packet is transmitted to the user which expects an answer, and a response is received, and if the response is valid, i.e. the user passes the authentication check, the connection attempt is granted and in an event the response in invalid, the connection is terminated, i.e. blocked, as evidenced by the reproduced section (col. 9 L5-67):

If, however, the ACL reply demands authentication, the agent should proceed to **106** and prompt for the user name. Note that some services such as gopher and WAIS do not provide a means to ask for a user name. In this case acid would have rejected the connection at the initial ACL check (because NSS **70** set the warder name to "none").

In one embodiment, a "magic window" is opened outside of the regular service to authenticate services like gopher and WAIS. In one such embodiment, a successful authentication will open a timed window to those services to allow access.

The prompt for a user name should include a way to specify the name of the warder. For example:

login: alan
login: alan:securid
login: alan:snk
login: alan:lockout
login: alan:fortezza
login: alan:password

Once the agent knows the user name, it should move to **108** and do a second ACL check. The query parameters in the second check should include the same parameters as the first check plus the name of the user. It should also include the name of the selected warder (if the user specified one).

If the reply to the second check says "deny" the agent should move to **110** and drop the connection. The agent may, however, want to first issue a dummy password/challenge prompt to avoid leaking information.

If the reply to the check says "allow," the reply parameters will include a list of allowed warders for that user. The agent should make sure that the user's selected warder is in the list of allowed warders. (If the agent passed the name of the selected warder to acid **60**, this test is done automatically by acid **60**.)

If the user did not select a warder, the agent should pick the first warder in the list of allowed warders and proceed to **112** to authenticate the user. At this point the agent is done making ACL checks. (In one embodiment, a menu of available warders is displayed for the user and the user selects one of the warders from the list of available warders. In such an embodiment, however, in order to prevent information leakage all warders should be listed, even those that do not actually apply.)

At **112**, the agent authenticates the connection with the selected warder. The agent should contact the selected warder and perform the authentication. This may include a challenge/response sequence. Please note that if the user changes his/her login name while talking to the warder, the agent must recheck the ACL with the new user name.

A check of the results of the authentication is made at **114** and, if at **114** the user passes the authentication check, the agent proceeds to **104**. If, however, the user fails the authentication check, the agent proceeds to **110** and drops the connection.

In short, the challenge as in the claims can be interpreted to be equivalent to the challenges disclosed in Stockwell due to the fact that both challenges require and/or expect a

response. More specifically, both challenges have same purpose and/or functionality, which is to grant and/or to deny the Internet access.

Stockwell also discloses reassessing the connection over a period of time. In other words, Stockwell teaches re-performing the ACL checks and authentication procedures after a time interval. The authentication procedure if demanded through ACL check will enable another set of challenge/response to be executed. Based on the response(s), the connection/access can be granted and/or terminated.

Based on the technical and/or logical line of reasoning, Stockwell discloses determining whether the client computer remains in compliance with ACLs for period of time as driven by the time intervals associated with the ACL rules. In other words, by periodically initiating an ACL check procedure, which may demand authentication, i.e. challenge/response sequence, the authenticator module determines whether the client computer remains in compliance with the authentication rule or policy.

However, in order to present a proper prima facie case, Phillips was introduced.

Phillips et al.

Phillips explicitly and/or clearly discloses transmitting plurality of challenges, i.e. same challenge as in Stockwell, over a period of time to each client computer, as evidenced by the following reproduced section:

PPP supports the Challenge Handshake Authentication (CHAP) protocol, which is designed for inclusion in PPP stacks. Authentication protocols are often employed to verify that users attempting to access a particular service are authorized users. For an example, the IWF 22 may wish to verify that the user of the TE2 device 12 is an authorized user of Internet access service offered via the IWF 22.

CHAP is often employed to improve the security of the communications link between two communications devices employing PPP protocols. CHAP is included in most PPP implementations and so is expected to be found in the PPP stacks on the communications devices. PPP also defines an extensible Link Control Protocol, which allows negotiation of an authentication protocol for allowing an authenticator to authenticate a peer before allowing network layer protocols to transmit over the link.

The authenticator is generally defined as the end of the link requiring the authentication. The authenticator indicates the employed authentication protocol via a Configure-Request message sent during a PPP link establishment phase. The end of the point-to-point link that is being authenticated by the authenticator is called the peer.

A CHAP authenticator sends a random challenge to a peer. The peer responds with a hashed response based on the challenge and a shared secret. To establish communications over a PPP link, each end of the PPP link sends LCP packets to configure the link during the PPP link establishment phase. An authentication phase follows the establishment of the PPP link. A network-layer protocol phase follows the authentication phase.

If authentication of the link is desired, a PPP implementation must specify the authentication-protocol configuration option during the PPP link establishment phase. CHAP periodically verifies the identity of the peer using a 3-way handshake upon initial link establishment and at random times during the establishment of the link.

After the link establishment phase is complete, the authenticator may send a challenge message to the peer. The peer responds with a value calculated using a one-way hash function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated. At random intervals, the authenticator may send a new challenge to the peer, repeating the above steps.

That is, at random intervals, the authenticator may send a new challenge to the peer, repeating the above steps, i.e. repeating: receiving a response, checking the response and terminating and/or acknowledging the authentication based on the response.

As such, the sending of challenges over random intervals, i.e. over a period of time, by itself, determines whether a given client computer remains in compliance with the access policy, i.e. user must be authorized and/or authenticated.

Therefore, the combination of Stockwell and Phillips and/or Stockwell does teach the method as in the pending claims.

a. (i). Appellant's claimed invention, which issues periodic challenges to client computers (i.e. user's computer), **requires** that a given client computer **remain** in compliance with the specified access policy (during a relevant period of time). Importantly, the concern addressed by the appellant's invention is a computer's continued compliance with applicable security policies (e.g. that it complies with a corporate security policy's requirement that a user's machine have up-to-date antivirus software), not its authentication or identity (e.g. username and password) (Brief, pg. 10).

In response to argument a (i), Examiner disagrees.

Independent claim 1 recites:

> In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on **a specified access policy (i.e. a rule set by the administrator, e.g. brief, pg. 10 lines 2-4)**, the method comprising:
>
> transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer, **for** determining whether a given client computer remains in compliance with **said specified access policy during said period of time;**
>
> transmitting a response from at least one client computer back to said client premises equipment for responding to each of said challenges that has been issued; and
>
> blocking Internet access for any client computer that does not respond appropriately to any challenge issued to it.

First, there is no teaching and/or suggestions of **requiring** a given client computer to **remain** in compliance with the specified access policy. In fact, the claim suggests that the client

computer may not comply and/or may become incompliant with the access policy, thus blocking the Internet access.

Secondly, there is no teaching and/or suggestion of a computer's **continued compliance** with the applicable security policies (e.g. that it complies with a corporate security policy's requirement to have up-to-date antivirus software…). In fact, the claim suggests that the client computer may not comply and/or may become incompliant with the access policy during a period of time, thus blocking the Internet access.

As such, the client computer does not remain and/or continue to remain in compliance.

Moreover, there are no teachings and/or suggestions whatsoever in the CLAIMED INVENTION of the fact that **one of the security policy's requirement is to have up-to-date antivirus software**. None of the claims, i.e. independent or dependent claims, discloses the usage of up-to-date antivirus software policy. Again, appellant is impermissibly importing the specification into the claims. It appears that appellant is addressing and/or focusing solely on the filed specification rather than the claimed invention.

At best, the claims, i.e. independent and/or dependent claims, recite the usage of "applications". **These applications do not disclose any antivirus software policy**.

For example:

The recited "applications", e.g. claim 11, can be interpreted as ftp and/or http applications. In other words, the Internet access is regulated in view of "applications" used to access the Internet.

Stockwell discloses the process wherein said access policy specifies which applications are allowed Internet access (col. 5 L16-22, col. 7 L1-45, col. 8 L20-30: ftp and http type of

accesses, col. 10 L12-67: Matching criteria for rule including: a list of service names such as ftp or http, in other words, a list of applications).

In other words, Stockwell discloses regulating the internet access/connection based on applications.

Third, prima facie case of obviousness is not rebutted by merely recognizing additional advantages or latent properties present in the Prior Art. Mere recognition of latent properties in the prior art does not render nonobvious an otherwise known invention. In re Wiseman, 596 F.2d 1019, 201 USPQ 658 (CCPA 1979)

"The fact that appellant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious." Ex parte Obiaya, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985) (The prior art taught combustion fluid analyzers which used labyrinth heaters to maintain the samples at a uniform temperature. Although appellant showed an unexpectedly shorter response time was obtained when a labyrinth heater was employed, the Board held this advantage would flow naturally from following the suggestion of the prior art.). See also Lantech Inc. v. Kaufman Co. of Ohio Inc., 878 F.2d 1446, 12 USPQ2d 1076, 1077 (Fed. Cir. 1989), cert. denied, 493 U.S. 1058 (1990) (unpublished — not citable as precedent) ("The recitation of an additional advantage associated with doing what the prior art suggests does not lend patentability to an otherwise unpatentable invention."). In re Lintner, 458 F.2d 1013, 173 USPQ 560 (CCPA 1972) and In re Dillon, 919 F.2d 688, 16 USPQ2d 1897 (Fed. Cir. 1990) discussed in MPEP § 2144 are also pertinent to this issue. See MPEP 2145 II.

In this case, Phillips explicitly discloses transmitting plurality of challenges over a period of time from client premises equipment to the client computer, as evidenced by the reproduced section (col. 5 L26-64):

PPP supports the Challenge Handshake Authentication (CHAP) protocol, which is designed for inclusion in PPP stacks. Authentication protocols are often employed to verify that users attempting to access a particular service are authorized users. For an example, the IWF **22** may wish to verify that the user of the TE2 device **12** is an authorized user of Internet access service offered via the IWF **22**.

CHAP is often employed to improve the security of the communications link between two communications devices employing PPP protocols. CHAP is included in most PPP implementations and so is expected to be found in the PPP stacks on the communications devices. PPP also defines an extensible Link Control Protocol, which allows negotiation of an authentication protocol for allowing an authenticator to authenticate a peer before allowing network layer protocols to transmit over the link.

The authenticator is generally defined as the end of the link requiring the authentication. The authenticator indicates the employed authentication protocol via a Configure-Request message sent during a PPP link establishment phase. The end of the point-to-point link that is being authenticated by the authenticator is called the peer.

A CHAP authenticator sends a random challenge to a peer. The peer responds with a hashed response based on the challenge and a shared secret. To establish communications over a PPP link, each end of the PPP link sends LCP packets to configure the link during the PPP link establishment phase. An authentication phase follows the establishment of the PPP link. A network-layer protocol phase follows the authentication phase.

If authentication of the link is desired, a PPP implementation must specify the authentication-protocol configuration option during the PPP link establishment phase. CHAP periodically verifies the identity of the peer using a 3-way handshake upon initial link establishment and at random times during the establishment of the link.

After the link establishment phase is complete, the authenticator may send a challenge message to the peer. The peer responds with a value calculated using a one-way hash function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated. At random intervals, the authenticator may send a new challenge to the peer, repeating the above steps.

CHAP packets may be framed and re-framed in the MT2 device **14** without departing from the scope of the present invention. In this case, the unframed CHAP packets are

That is, after the link/connection is established, then, at random intervals, the authenticator may send a new challenge to the peer, receive a response, check the response and allow/terminate the connection based on the response. In other words, plurality of challenges are transmitted to the client over a period of time, e.g. every 60 seconds and/or every random seconds, a challenge is sent, in order to improve the security of the communication, as seen above.

This teaching, by itself, determines whether the peer device **remains in compliance** with the access policy and/or rule such as only authorized users are granted access, wherein the authorization is performed through authentication comprising challenge/response sequence.

For example: In this case, the access policy can be in such a way that the user must be authorized, or must be in authorized list or must be authenticated for accessing the network or Internet. In other words, access is granted only if the user is authorized, and continued to be granted if the user continues to respond appropriately to the random challenge, otherwise, the connection is terminated. The process of determining whether the user is authorized is performed through authentication that comprises challenge/response sequence. At random interval, a challenge is sent to the user, a response is received and validated. Based on the response, the connection/access can be terminated and/or acknowledged. This process can continually continue at random intervals, thus determining whether the client computer remains in compliance with the access policy.

In other words, the determination of the continued compliance naturally flows from transmitting plurality of challenges over a period of time.

a. (ii) Authentication protocols…are well known in the art…Instead, the particular issue addressed by the appellant's invention is to make sure that a client-side security module is both installed and properly operating one ach local computer. Here the "properly operating" means that each client computer not only has the client-side security module installed but each computer is continually checked to make sure it is operating pursuant to security policies...Succinctly stated appellant's invention is continually...issues challenges to a client computer **for determining whether the client computer is in compliance with the above-described access policy**…(Brief, pg. 10-11: Last paragraph).

In response to argument a. (ii), Examiner respectfully disagrees.

Again, it's clearly seen that appellant, impermissibly, imports and/or reads the limitations from the specification into the claims. For example: security module is both installed and properly operating…properly operating means that…etc.

It is noted that these features upon which appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As per "…for determining…", it should be noted that prima facie obviousness is not rebutted by merely recognizing additional advantages or latent properties present in the Prior Art. Mere recognition of latent properties in the prior art does not render nonobvious an otherwise known invention. In re Wiseman, 596 F.2d 1019, 201 USPQ 658 (CCPA 1979)

"The fact that appellant has recognized another advantage **which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when**

the differences would otherwise be obvious." Ex parte Obiaya, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985) See also Lantech Inc. v. Kaufman Co. of Ohio Inc., 878 F.2d 1446, 12 USPQ2d 1076, 1077 (Fed. Cir. 1989), cert. denied, 493 U.S. 1058 (1990) (unpublished — not citable as precedent) ("The recitation of an additional advantage associated with doing what the prior art suggests does not lend patentability to an otherwise unpatentable invention."). In re Lintner, 458 F.2d 1013, 173 USPQ 560 (CCPA 1972) and In re Dillon, 919 F.2d 688, 16 USPQ2d 1897 (Fed. Cir. 1990) discussed in MPEP § 2144 are also pertinent to this issue.

As set forth above, in Phillips, plurality of challenges are transmitted to the client over a period of time, e.g. every 60 seconds a challenge is sent, e.g. Phillips: col. 5 L26-64.

This teaching, by itself, determines whether the peer device **remains in compliance** with the access policy and/or rule as set forth above.

In other words, the continual compliance and/or determining whether the client computer remains in compliance with access policy **naturally flows** from transmitting plurality of challenges over a period of time.

Appellant throughout the brief asserts that appellant's invention does not provide authentication services, e.g. brief, pg. 10, however, appellant fails to note that the pending claims clearly read on an authentication protocol and/or policy, and further asserts that "what is needed is a solution that requires the user to have his or her computer come into compliance and stay in compliance at all relevant times…", e.g. brief, pg. 11: last paragraph.

However, there is no teaching and/or suggestion in the claimed invention of such a solution.

Authentication protocol governs the access, whether it is network or internet, based on access policy as driven by authorized lists that lists the users authorized to access. The authorized users are confirmed through challenge-response sequence that may use the username and password, See for example, MS Computer Dictionary, Fifth Edition, ISBN 0-7356-1495-4, pg. 42.

Moreover, appellant's specification discloses (pg. 28 line 6 to pg. 29 line 10):

> "…may connect to the LAN or to the Internet. **The administrator or user may use this allow** connect column 533 to allow access (indicated by a check mark in this column), to deny access (indicated by an X) **or to ask for specific authorization (indicated by a question mark).** For example, for the first program shown in the program list column 532 named "CyberKit," the allow connect column 533 is set to ask the administrator **or user for specific authorization each time the program connects to the LAN** or Internet. The allow server column 534 enables the administrator or user to control which programs can perform server functions. The options column 535 provides additional options for establishing the permitted activities of each program."

In other words, the administrator can set the policy to ask for specific authorization. More specifically, the specification discloses asking the user for specific authorization. This authorization can be via challenge/response techniques of Stockwell and Phillips.

Moreover, appellant acknowledges the usage of rules in Stockwell, e.g. Brief, pg. 9 3rd paragraph).

a. (iii) Significantly, appellant's...for example: the system admin...a policy requiring that a specific version of the security solution or a specific virus protection program is operational on each...again note that authentication...(Brief, pg. 12).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a policy

requiring that a specific version of the security solution or a specific virus protection program is operational on each) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

On page 12 of the brief, appellant asserts that "Instead of repeatedly…Every few second appellant's router-side client management protocol component sends out a communication via Internet broadcast…that is described as router challenge. **This router challenge – which is repeatedly initiated by the router and not by the user or his/her computers** -- requires a response from..."

In view of the specification and/or claims, Examiner disagrees with the appellant's assertion that the router challenge is not repeatedly initiated by the user or his/her computer. In fact, claims 5-6 explicitly discloses that this router challenge is initiated by the client computer by sending a client hello packet to the client premises equipment.

Appellant further asserts that "any computer that does not have the client-side security module installed or is otherwise noncompliant… is unable to respond to the router challenge in an appropriate manner, and this will...", e.g. brief, pg. 13.

Again, the "any computer that does not have the client-side security module installed or is otherwise noncompliant… is unable to respond to the router challenge in an appropriate manner" are not recited in the claims. Appellant is clearly, impermissibly, importing the specification into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As per "appellant's approach's advantages", the rejection and/or combination of references, i.e. Stockwell and Phillips, also provides an advantage that a given client computer must at all times be able to establish – and continue to re-establish – its compliance with required access policy. The moment a computer falls out of compliance, e.g. due to incorrect username and password, it is blocked from access. E.g. Stockwell: col. 9 L60 to col. 10 L8 and Phillips: col. 5 L26-64.

Appellant also asserts that Phillips patent does not even mention the words "compliance" and "policy"…e.g. brief, pg. 13. On the other hand, appellant admits that authentication protocol is well known in the art, e.g. brief, pg. 10.

In view of authentication techniques, the terms "compliance" and "policy" are very well known to the one of ordinary skilled in the art. The policy can simply mean that access is only granted to authorize users and compliance simply means adherence to the policy. One way to authorize the users of a computer are through challenge/response protocol as set forth above.

a. (iv) Appellant's invention does not permit or block requests for access based on user login or other authentication information. Instead, appellant's system determines whether a given client computer is in compliance with the specified access policy governing internet access (Brief, pg. 13).

In response to argument a. (iv), Examiner disagrees.

An access policy can be defined in terms of authentication and/or authorization. One way to determine whether the user is authorized to access the Internet or network is through challenge/response sequence which may use username and password. If the username and

passwords, i.e. response to challenge, are incorrect, access is denied, i.e. user is not authorized to access the network/Internet and/or user is not on authorized list. If the username and password, i.e. response, are correct, then access is granted, i.e. the user is authorized user.

Appellant fails to note that the appellant's claimed method and/or system determines whether a given client computer is in compliance with the access policy governing internet access, is in fact, based on sending a challenge and receiving a response. More specifically, the claim discloses blocking/granting access based on the response in view of challenge.

There are no teachings and/or suggestions that explicitly show that the challenge as in the present claims is not equivalent to and/or cannot be interpreted as the challenge(s) of Stockwell and Phillips. **Moreover, the pending claim does not disclose that the challenge-response is not based on login or other authentication information.**

In conclusion, appellant asserts that "appellant's claimed invention provides around…".

In summary, it should be noted that these alleged features are not disclosed in the CLAIMED INVENTION. Appellant is, impermissibly, reading and/or importing the limitations from the specification into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As set forth above, e.g. pg. 15-21 of this action, the combination of Stockwell and Phillips does disclose the method as in the claimed invention.

b. Second Grounds of Rejection (Brief, pg. 15).

In the Brief, e.g. pg. 15, appellant asserts that "moreover…this is not appellant's claimed approach. Appellant's approach provides for making the decision about whether or not to permit access based on a client compute's "then-current compliance" with any applicable access policy.

In response to appellant's assertions, Examiner disagrees.

First, it is unclear what "then-current compliance" means and/or what appellant is trying to disclose.

Secondly, the "then-current compliance" with any applicable policy is not recited in the claims. The claim merely refers to "access policy".

Furthermore, appellant asserts that "the client hello limitation of the rejected claims...make it clear that appellant's claimed approach is directed to device-to-device (i.e. router to computer) compliance verification irrespective of what the user is doing. The combined references do not teach this limitation".

In response to appellant analysis, the device-to-device verification **irrespective** of what the user is doing is not recited and/or suggested in the claims. Moreover, Kadyk reference discloses the SAME "client-hello" packet, e.g. col. 10 L20-52, in order to establish the connection, which can include challenge/response sequence.

c. Third Grounds of rejection (Brief, pg. 16).

In the Brief, e.g. pg. 16, appellant asserts that "moreover…this is not appellant's claimed approach. Appellant's approach, as set forth in these rejected claims, provides for determining whether or not to permit Internet access based on compliance with an access policy which specifies particular applications which are approved for Internet access. "Particular applications" in this context may mean that a certain version (namely, the latest up-to-date version) of antivirus software must be installed, for example. The combined references have no facility to predicate access on the basis that certain software be installed on the client computer.

In response to appellant's assertions, Examiner disagrees.

In response to appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., Particular applications may mean a certain version of antivirus software must be installed) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Moreover, in view of specification, e.g. pg. 29 lines 14-31, these particular applications may comprise real player, user-defined applications, etc.

As set forth above, at best, the claims, i.e. independent and/or dependent claims, recite the usage of "applications". **These applications do not disclose any antivirus software policy**.

For example:

The recited "applications", e.g. claim 11, can be interpreted as ftp and/or http applications. In other words, the Internet access is regulated in view of "applications" used to access the Internet.

Stockwell discloses the process wherein said access policy specifies which applications are allowed Internet access (col. 5 L16-22, col. 7 L1-45, col. 8 L20-30: ftp and http type of accesses, col. 10 L12-67: Matching criteria for rule including: a list of service names such as ftp or http, in other words, a list of applications).

d. Fourth Grounds (Brief, pg. 17).

Examiner disagrees for the same reasons as set forth above. More specifically, Stockwell-Phillips and Shrader discloses redirecting to a sandbox server, e.g. see rejection of claims 1 and 22 above. Importantly, the claim does not suggest and/or teach that the redirection is not on the lack of authentication of the user.

e. 35 USC 112, second paragraph rejections (Brief, pg. 17-18 E: Fifth ground).

In response to appellant's argument [e], Examiner withdraws the rejection in view of appellant's arguments as on pg. 17-18 of brief.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Kamal Divecha
Art Unit 2451
/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451

Conferees:

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446